Malware: Beware of Email Attachments

Don’t Trust to Luck! Learn How to Recognise Malicious Email Attachments

This article shows you how to:

- Spot fake file extensions in the names of attachments
- Be wary of attachments sent in zip files
- Check an attachment with over 60 anti-malware scanners

My friend sent me a funny photo by email, but when I tried to open it, my anti-virus program warned me about it. Was this just a false alarm, or is it possible the photo really was dangerous?

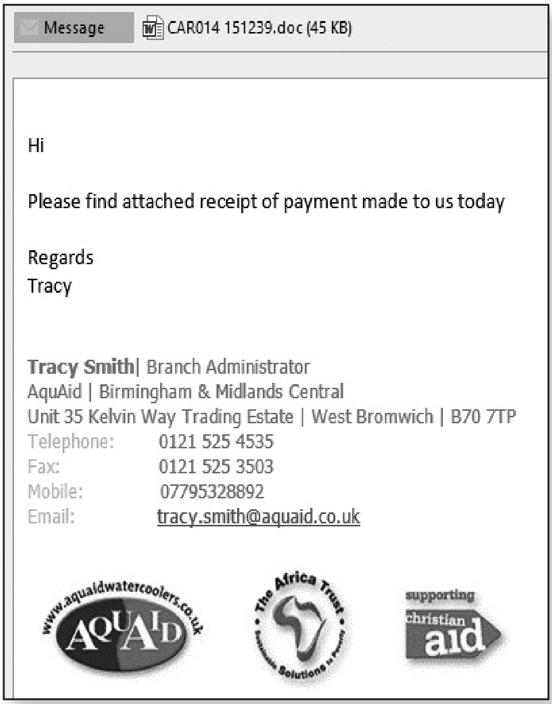
This is a question we were asked recently, and the questioner was lucky. The email message wasn’t really sent by his friend, and the attachment wasn’t really a photo. Find out how to recognise dangerous email attachments without taking the risk of opening them.

Contents:

The Dangers of Malicious Email Attachments

Who has taken your money?

You’ve just received the email message pictured below, and you’re puzzled by it. You know you haven’t made a payment to this company – at least, not intentionally – but why does it think you have? Has the company somehow got hold of your credit card details? How much have you paid?



Hi

Please find attached receipt of payment made to us today

Regards
Tracy

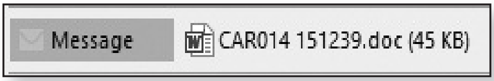
Tracy Smith| Branch Administrator
AquAid | Birmingham & Midlands Central
Unit 35 Kelvin Way Trading Estate | West Bromwich | B70 7TP

Telephone:	0121 525 4535
Fax:	0121 525 3503
Mobile:	07795328892
Email:	tracy.smith@aquaid.co.uk

The attachment claims to tell you

The message itself looks credible. It’s laid out neatly, it includes the company’s contact details, and those logos make it look trustworthy. The problem is that it doesn’t tell you anything useful. Clearly, to find out what’s going on, the only option is to open the attached file.

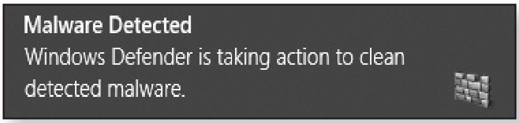
A glance at the attachment tells you it's a Microsoft Word document: you can tell by the Word icon to the left of the filename and the '.doc' file extension.


Message CAR014 151239.doc (45 KB)

Surely a Word document is safe?

Even if you're generally cautious about attachments, you might well feel that a Microsoft Word document is safe for you to open: surely it just contains harmless text? But perhaps your confusion and concern about what's going on would lead you to open the attachment without even considering whether it's safe or not.

Well, I can show you what happens when I try to open this attachment on my own computer:


Malware Detected
Windows Defender is taking action to clean detected malware.

Not necessarily!

The Windows Defender program built into Windows has recognised this attachment as malware and prevented it from opening. The notification above pops up on my screen to tell me so.

This time I've been fortunate. But if it were a different email message and a different attachment, or an older and less-secure version of Windows, the outcome might well have been disastrous.

This attachment contains malicious software

The Microsoft Word document in this example certainly doesn't just contain harmless text. In fact, if you were able to open it, it would appear to be just a blank page. What it does contain is a hidden 'macro' – a type of small program that can be included in Word documents and other types of Microsoft Office files. This macro aims to infect your PC with a wide variety of malicious software designed to steal passwords and card payment details, and to encrypt your personal files and then start demanding ransom payments.

> Despite what happened to me in the example above, don’t assume that you can try to open any attachment you receive and rely on your anti-virus software (be it Windows Defender or something else) to protect you from anything that turns out to be harmful!
>
> In this case, I knew the attachment was malicious, but I also knew Windows Defender was going to catch it. If I hadn’t been certain of this, I wouldn’t have tried to open it!

How Scammers Trick Us into Opening Attachments

Scammers try to trick us

As I’m sure you’ve guessed, the email message wasn’t sent by the company named in the text. It was sent by scammers who hope we’ll be curious enough – or worried enough – to open the attachment.

Simply receiving an email message that contains a malicious attachment doesn’t do any harm. Therefore, the scammers need us to actually open that attachment, and they use several tricks to fool us into doing so:

Trick 1: Few details in the text

Just enough text to make you curious or worried

The message is usually very short, containing just enough information to make us curious or concerned, but making it clear that we’d have to open the attached file to learn more. It may well contain company details and logos, ‘small print’ and disclaimers – all the usual things we’d expect to see in a legitimate message from that company or organisation – designed to allay any suspicions we might have.

> Don’t let logos in email messages fool you! It only takes a minute to find and download the official logo of a company or organisation and pop it into an email message. To the scammers, that’s a minute well spent, because they know the effect it will have on some less-experienced computer users.

The fact that the message itself tells you so little should always strike you as suspicious. My earlier example was supposedly a receipt for payment, so why would they have sent the details as an attached file? Why not simply include them in the text of the message?

Examples of attachment scams

Exactly the same question applies to the other common types of email attachment scam:

- A parcel sent via Federal Express or DHL couldn’t be delivered to you. To find out who sent it, you’d have to open the attachment.
- There’s an important security warning sent from Microsoft. What’s it about? Only the attachment will tell you.
- Congratulations, your holiday has been booked. What holiday – and who paid for it? Find out by opening the attachment.
- You’ve just received a fax. How? From whom? And how on earth could it arrive by email? It sounds a bit silly, but perhaps you’d be curious enough to look at the attachment.
- A debt recovery firm is taking you to court for non-payment. You have one last chance to settle the debt. Who do you owe? And how much? You guessed it – you’d have to open the attachment.

If a message tells you just enough to arouse your curiosity, but wants you to open an attachment to learn anything useful, you can be sure it’s a scam and that attachment is going to be dangerous. If you keep this in mind, the remaining three tricks should stand little chance of success!

Trick 2: Filenames with double extensions

Only the second file extension matters!

This is a ploy designed to make you believe that the file you've been sent is safe – that it's a type of file that couldn't possibly harbour malicious software. For example, you might well think it's a harmless photo because the file's extension (the characters following the dot in its name) seems to be **.jpg**, which is the well-known file extension of JPEG pictures.

Scammers add two extensions to the filename, such as **.jpg.exe**. In some cases, you might only see the first extension (**.jpg**), assume it's a photo and open it, unaware that the real extension is **.exe**, which denotes a program. I'll explain more about this trick and how to avoid it on page 7.

Trick 3: Sending malicious programs in zip files

Malicious programs can be sent in zip files

What scammers want to send you are programs, because a program has the best chance of infecting your computer. However, they can't do that easily. Your email service would usually strip out any programs that arrived for you in email messages, and your email program should prevent you from accessing any that did get through.

Instead, scammers put the malicious program into a zip file and send that as an attachment. The zip file will usually reach you intact. The question is, can you be fooled into opening the zip file and then opening the file you find inside it? We'll look at this in more detail on page 8.

Trick 4: Sending files which look harmless

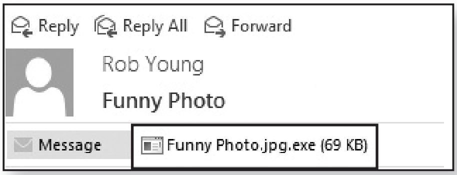
Some safe-looking files could be dangerous

Many computer users know that programs and a few other types of file are potentially harmful, and nothing would convince them to open one of those files if it arrived as an unexpected email attachment. However, they might willingly open other types of file in the belief that they couldn't possibly contain anything malicious. One example is a Microsoft Word document, as we encountered on page 3 of this article. I'll point out the potentially-harmful types of file on page 12.

Beware of Double File Extensions!

A filename with two extensions

Have a look at the name of the attached file in the screenshot below. What type of file would you say it is?



A JPEG photo?

The name of the file, 'Funny Photo', suggests it's a picture, and straight after the name you see **.jpg** which you might recognise as the file extension denoting a JPEG picture file.

No, it's a program

In this case, though, '.jpg' is not the file extension. Straight after that there's another extension, **.exe**, and it's always the very last extension that matters: the file extension is what follows the very last dot in a filename.

Here, then, the file extension is **.exe**, which is the extension that denotes a program. If you were to open this attachment in the belief that it's a photo (and if your anti-virus software allowed it to open), you could be in serious trouble!

Scammers use this 'double extension' trick to try to fool you into believing that a file is safe to open. The first extension denotes something ordinary and innocent such as **.jpg** (a photo), **.txt** (a plain text file) or **.mp3** (an audio/music file), and the scammer hopes you'll latch on to that and ignore the fact that there's another extension following it.

Always look at the last extension!

Unlike files you see elsewhere in Windows, modern email programs always display the full filename, including the file extension, so be sure to look at what follows the last dot in the name in order to identify what type of file it really is.

If you're using an old email program, it pays to find out whether or not it displays file extensions. An easy way to do that is to find an email message you were sent by someone trustworthy: perhaps a friend has sent you a photo which you kept, for example. Open that message and look at the name of the attachment: if you can see the file extension after its name, you know your email program does display file extensions. Therefore, if you receive a scam message using this 'double extensions' trick, you know you'll see both extensions.

If you discover that your email program doesn't display extensions, remember that! If you receive an attachment whose name does show an extension (such as **Funny Photo.jpg**), there's something fishy about it! You know that your email program doesn't display extensions, which can only mean that there's another, hidden extension after this one. You don't know what this hidden extension is, but the fact that there is a second extension tells you immediately that someone is trying to fool you.

Be Suspicious of Attached Zip Files!

Email services reject programs sent by email

From the scammers' point of view, the surest way of infecting your PC with malware is by sending you a program and fooling you into running it. However, as

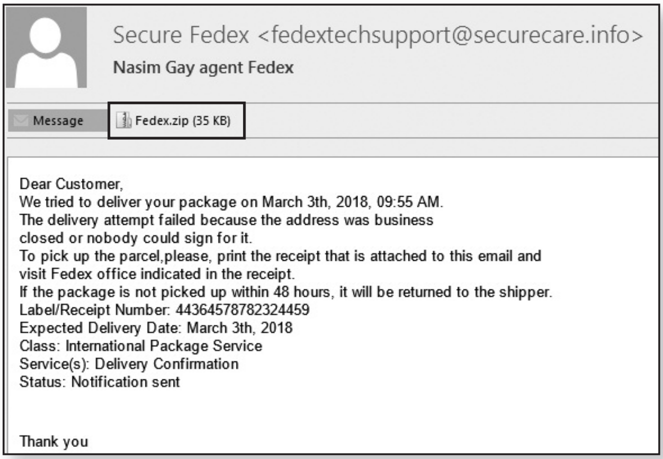
I mentioned earlier, that's not easy to do nowadays. If the scammer simply attaches a program to his email message, it will usually be stripped out by your email service or email program.

Scammers enclose programs in a zip file

What the scammer does instead is to send you a zip file containing the malicious program. A zip file is an odd type of file which is designed to hold one or more other files, rather like a folder. (Indeed, Windows refers to zip files as 'Compressed Folders'.) To your email service and email program, this zip file looks quite innocent: they don't examine what's lurking inside it.

Example: parcel delivery scam

In the example below, Federal Express has apparently failed to deliver a parcel to me, and the message says I should print the receipt in the attachment. The attachment is a zip file named 'Fedex.zip'.


Secure Fedex <fedextechsupport@securecare.info>
Nasim Gay agent Fedex

Dear Customer,
We tried to deliver your package on March 3th, 2018, 09:55 AM.
The delivery attempt failed because the address was business
closed or nobody could sign for it.
To pick up the parcel,please, print the receipt that is attached to this email and
visit Fedex office indicated in the receipt.
If the package is not picked up within 48 hours, it will be returned to the shipper.
Label/Receipt Number: 44364578782324459
Expected Delivery Date: March 3th, 2018
Class: International Package Service
Service(s): Delivery Confirmation
Status: Notification sent

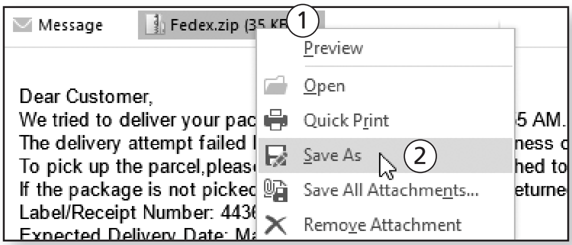
Thank you

It's not difficult to spot that this is a scam. For one thing, how many of us receive parcels via FedEx? For another, your email program would probably put this straight into your Junk folder, as mine did, which tells you it's unlikely to be legitimate. For a third, if FedEx really had tried to deliver a parcel to you, they'd know your name – so you wouldn't be 'Dear Customer' – but how on earth could they know your email address?

See what's inside the zip file

But this is just one example of many, so let's overlook its obvious failings and pretend that we're not yet sure whether it's a scam. Follow these steps to find out what's inside that zip file:

1. The first thing to do is to save the attached zip file to your computer, where you can open it and look inside it. In most email programs, you do that by right-clicking the attachment ① and choosing **Save As** ②, then choosing which folder you would like save it in. (Choosing **Desktop** is recommended, so that the the file will then be easy to find.) An alternative way to save the attachment is to use the left mouse button to drag it out of your email program and drop it on the desktop.



Dear Customer,
We tried to deliver your pac
The delivery attempt failed l
To pick up the parcel,pleas
If the package is not pickec
Label/Receipt Number: 443
Expected Delivery Date: M

5 AM.
ness c
hed to
eturne

2. Next, double-click the zip file you've just saved and Windows will open it to show you the file stored inside it.

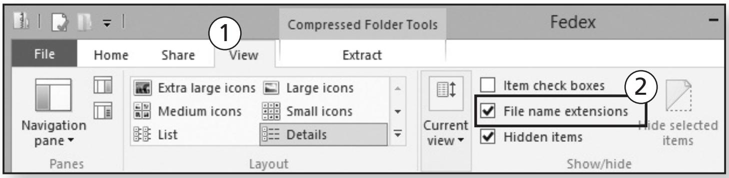
From this point onwards, be careful! If you were to double-click the file that's stored inside this zip file, Windows would open it. You don't yet know what type of file it is or whether it could be malicious, and you don't know whether your antivirus software would protect you from it, so double-clicking it could spell disaster!

Make Windows display file extensions

3. Now let's find out what kind of file you've been sent. To do this, we need to tell Windows to display file extensions, which are currently hidden. Here's what to do:

   Windows 11: click the **View** button on the toolbar, move the mouse down to **Show** and click on **File name extensions**.

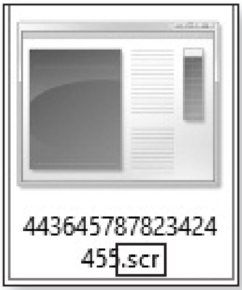
   Windows 10 or 8.1: switch to the **View** tab on the Ribbon ①, and in the 'Show/hide' section tick the box beside **File name extensions** ②.



   Windows 7: press the **Alt** key on your keyboard to display the menu bar at the top of the window, then open the **Tools** menu and choose **Folder Options**. In the dialog that opens, switch to the **View** tab. In the list of options, remove the tick beside **Hide extensions for known file types** and then click **OK**.

Look at the file extension

4. Now Windows will show you the file extension of the file inside that zip file alongside its name. Have a look at the extension and, if you don't recognise it, look for it in the list of dangerous extensions on page 13. In the case of the 'Fedex' zip file I've received, I can now see that the file extension is **.scr**, which denotes a screen saver. This means the file is a type of program – not the document or 'receipt' that was mentioned in the



email message, and certainly not something I'd risk opening!

Remember that scammers may use the 'double extension' trick with the file inside this zip. If you follow step 2 above and discover that you can already see a file extension at the end of the filename, don't be fooled by it! Continue following steps 3 and 4 and you'll find that there's a second extension which, as always, is the one that tells you what type of file you're really dealing with.

Hide file extensions again

Having seen the extension of this file, you'd probably like to tell Windows to hide file extensions again. To do that, repeat step 3 and remove the tick beside **File name extensions** in Windows 11/10/8.1, or tick the box beside **Hide extensions for known file types** in Windows 7.

Which File Extensions Can Be Dangerous?

Check whether a file could be malicious

At this point, you know the various tricks used by scammers to get malicious files to you as email attachments. You also know how to determine the file extension of the attached file, even if the scammer is trying to fool you by using two extensions, and/or by sending it in a zip file.

The question now is: what kind of file have you been sent? Let's run through the file extensions you should always treat as suspicious. They divide into two main categories:

High-risk files: never open these!

Never a good reason for sending these files by email

The file extensions in the table below denote programs and similar files. Of course, programs are not always dangerous – your PC would be no use for anything at all if you couldn't use programs! – but they can be. However, there is no legitimate reason for anyone to send you one of the following files by email, so if you ever receive one, you should always assume the file is dangerous.

File extension	Type of file
.bat	A batch file containing Windows commands.
.com	An old type of MS-DOS program.
.cpl	A Control Panel program.
.exe	A Windows program.
.inf	An installer file which could damage your system.
.jar	A Java program.
.js/.jse	Script files containing Windows commands.
.msi	An installer file which installs a program on your computer.
.pif	An old type of MS-DOS program.
.reg	A Registry file which could add or delete details from the Registry.
.scf	A script file containing Windows commands.
.scr	A Windows screen saver program.
.vb/.vbe/.vbs	Script files containing Windows commands.
.ws/.wsc/.wsf/.wsh	Script files containing Windows commands.

Potentially-dangerous files

These files could contain malware

Our second group of file extensions contains files you might receive regularly from friends, family and other trusted sources (and you might send them yourself). However, files with these extensions can be used to infect your computer with malicious software, so you should always consider carefully whether you trust the sender of the email message before opening one of these:

File extension	Type of file
.doc/.docx/ .docm	Microsoft Word documents. These can potentially contain small programs named ‘macros’ which could be harmful.
.dot/.dotx/ .dotm	Microsoft Word template files. Can contain macros, as above.
.pdf	A PDF document. These can take advantage of security flaws in Adobe Reader to install malicious software.
.ppt/.pptx/ .pptm	Microsoft PowerPoint slideshow files. Can contain macros, as above.
.rar	Similar to a zip file (see .zip below).
.xls/.xlsx/.xlsm	Microsoft Excel spreadsheets. Can contain macros, as above.
.xlt/.xltx/.xltm	Microsoft Excel template files. Can contain macros, as above.
.zip	A zip file (or ‘Compressed Folder’) containing one or more files. Commonly used to send malicious software as an email attachment.

Safely Check an Attachment Without Opening It

Enough clues to be sure the file is dangerous?

As you’ve learned over the preceding pages, scammers use a variety of tricks to disguise the malicious software they send you, but there are methods you can use to learn more about what you’ve received. In many cases, too, simply looking at the text, subject and sender of the message is enough to make you certain that the attachment will be something malicious.

Sometimes, though, you’re not quite sure. For example, perhaps you’ve received an email attachment that appears to have come from a friend or relative, or from a company or organisation whose name you recognise, but something about it doesn’t seem quite right.

Not sure? Scan it at VirusTotal

Don’t take any chances! If there’s the slightest doubt in your mind, take a couple of minutes to follow the steps below and have the attachment scanned using an excellent free service named VirusTotal:

1. Begin by saving the attached file to somewhere easily accessible, such as your desktop. You can do this by following step 1 on page 10. (Although that step refers to a zip file, it applies to any type of attached file.)

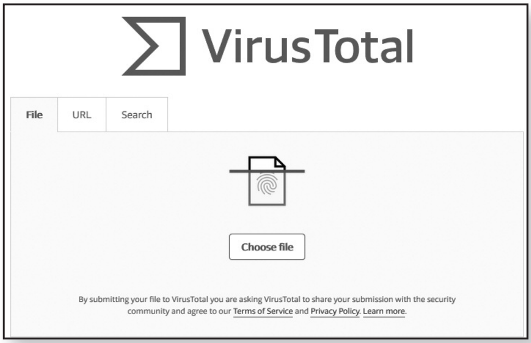
   Once you’ve saved the file to your desktop, be sure not to double-click it! Doing so would open the file, with possibly-disastrous consequences if it is malicious!

2. At this point, your anti-virus software might leap into action, either warning you about this file, deleting it or moving it to ‘quarantine’. If so, this confirms the file is dangerous; there’s nothing more to do but delete the email message you received.

3. Assuming your anti-virus software hasn’t removed the file, start your web browser and visit this address: www.virustotal.com.

Tell VirusTotal to scan the file

4. When the web page opens, click the **Choose file** button. This opens a ‘File Upload’ dialog: select the file you’ve just saved to your desktop and click **Open** followed by **OK**.



By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more.

VirusTotal might have seen it before

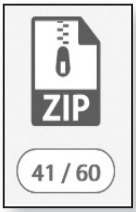
5. At this point you may see a pop-up headed ‘File already analysed’. If so, this means that someone else has already scanned this file using VirusTotal. (That suggests the same file has been sent to many people besides yourself, which already gives an indication that it’s probably malicious.) If so, click on **View last analysis** to start the process.

6. VirusTotal now scans your file using up to 67 different anti-virus programs – a combination of famous and not-so-well-known scanners.

Check the scan results

7. After a few seconds, you’ll see the results of all the anti-virus scanners in a list:

   - If a scanner did not find anything suspicious in your file, you’ll see a white tick in a green circle beside its name and the word 'Clean'.
   - If a scanner did find malware in the file, you’ll see the name of the malware in red beside the scanner’s name and a red warning icon.
   - At the top of the page you’ll see a note of how many of the anti-virus scanners regarded this file as dangerous (41 out of 60 in this example – a clear indication that the file I’ve just scanned isn’t to be trusted).



If it appears unsafe, delete it!

It’s rare that all 67 scanners will reach the same conclusion about the file, and different scanners use different names for the same malware. However, if the vast majority of these scanners found nothing suspicious, your file is almost-certainly safe. But if at least a handful found malware in it, take this seriously: delete the file from your desktop and delete the email message in which it arrived.